Internet of Things

ENOG 14, Minsk, BY, 2017-10-10

http://slides.cabo.space

Prof. Dr.-Ing. Carsten Bormann, cabo@tzi.org

Carsten Bormann

Universität Bremen TZI
IETF CoRE WG
IRTF T2T RG

http://slides.cabo.space

RFC 2429	RFC 2509	RFC 2686	RFC 2687	RFC 2689	RFC 3095
RFC 3189	RFC 3190	RFC 3241	RFC 3320	RFC 3485	RFC 3544
RFC 3819	RFC 3940	RFC 3941	RFC 4629	RFC 5049	RFC 5401
RFC 5740	RFC 5856	RFC 5857	RFC 5858	RFC 6469	RFC 6606
RFC 6775	RFC 7049	RFC 7228	RFC 7252	RFC 7400	RFC 7959
RFC 8132	RFC 8138				

Bringing the Internet to new applications

- "Application X will **never** run on the Internet"
- …
- …
- "How do we turn off the remaining parts of X that **still** aren't on the Internet"?

Internet of Things

Scale up:

Number of nodes

(xx billion by 2020)

Internet of Things

Scale down:

- node

Internet of Things

Scale down:

cost

complexity

cent

kilobyte

megahertz

Constrained nodes: orders of magnitude

10/100 vs. 50/250

There is not just a single class of "constrained node"

RFC 7228

Class 0: too small to securely run on the Internet

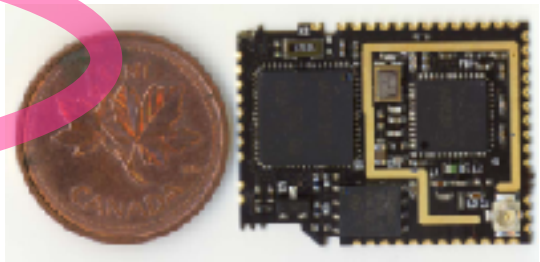
- ✘ "too constrained"

Class 1: ~10 KiB data, ~100 KiB code

- ✔ "quite constrained", "10/100"

Class 2: ~50 KiB data, ~250 KiB code

- ✔ "not so constrained", "50/250"



These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes

Internet of Things?

IP = *Internet* Protocol

“IP is important”

IP = *Integration* Protocol

IP: drastically reducing barriers

- **IP telephony** (1990s to 2018): replaced much of the special telephony hardware by routers and servers
  - several orders of magnitude in cost reduction
  - available programmer pool increases massively
  - What started as convergence,
    turned into **conversion**
- Everything is **not** the special snowflake it is said to be
- Now: **Internet of Things**

Hype-IoT	Real IoT
IPv4, NATs	IPv6
Device-to-Cloud	Internet
Gateways, Silos	Small Things Loosely Joined
Questionable Security	Real Security
$40+	< $5
W	mW, µW

IoT: Current Deployment Models

- **Device to cloud**
  - Add isolated nodes to existing LANs (e.g., WiFi)
  - Lots of “ants” (v4: You might see this in your CGNs)
  - v4: Reachability from outside requires keepalive (often UDP!)
- **Device to “gateway”**/hub (…to cloud)
  - Closer to other traffic we have today
  - Adds more periodic microflows to the mix
- **Device to device** (“thing-to-thing”, general Internet connectivity)
  - (v4: Behind the NAT, or lots of hole punching needed)

[RFC 7452]

> … a properly networked world … could be safer, greener, more efficient and more productive … But in order for that to emerge, the system has to be designed in the way that the internet was designed in the 1970s – by **engineers who know what they're doing**, setting the protocols and technical standards that will bring some kind of order and security into the chaos of a technological stampede.

John Naughton, "The internet of things needs better-made things"
(The Guardian, 2016-07-10)

I E T F®

IETF: Constrained Node Network WG Cluster

INT	LWIG	Guidance
INT	6LoWPAN ✔	IP over 802.15.4
INT	6Lo	IP-over-foo
INT	6TiSCH	IP over TSCH
INT	 LPWAN	Low-Power WAN Networks
RTG	ROLL	Routing (RPL)
APP	CoRE	REST (CoAP) + Ops
APP	 CBOR	CBOR & CDDL
SEC	DICE ✔	Improving DTLS
SEC	ACE	Constrained AA
SEC	COSE ✔	Object Security

Technology	Traits
IEEE 802.15.4 (“ZigBee”)	Many SoCs, 0.9 or 2.4 GHz, 6TiSCH upcoming
BlueTooth Smart	On **every Phone**
DECT ULE	**Dedicated Spectrum**, In every home gateway
ITU-T G.9959 (“Z-Wave”)	Popular @home
802.11ah (“HaLow”)	Low power “WiFi”
NFC	**Proximity**
6lobac	**Wired** (RS485)
IEEE 1901.2 (LF PLC)	Reuses mains **power** lines
Ethernet + PoE	**Wired**, supplies 12–60 W
WiFi, LTE, …	**Power?**

2.4 GHz

1.8 GHz

0.9 GHz

13.56 MHz

Application Layer Protocols

- CoRE: Constrained **REST**ful Environments:
  Replace HTTP by a less expensive equivalent (**CoAP**)
    - From special-purpose/siloed to **general purpose**
- ACE: Define Security less dependent on humans in the loop and on very fast upgrade cycles
    - Embrace the **multi-stakeholder** IoT

Application Layer Data Formats

- Industry move to **JSON** for data interchange
- Add **CBOR** where JSON is too expensive
- Use **JOSE** and **COSE** as the security formats
- Work on semantic interoperability (IRTF **T2TRG**), with W3C, OCF, OMA/IPSO (LWM2M), iot.schema.org, …
  ➔ self-description

Reducing TCO: Self-Description and Discovery

- Manually setting up 10^{11} nodes is a non-starter
- **Self-Description**:
  IoT nodes support automatic integration
  - RFC 6690 /.well-known/core "**link-format**"
  - W3C WoT work on "Thing Description" ongoing
  - **Semantic Interoperability**!
- **Discovery**:
  IoT nodes and their peers can find others
  - /.well-known/core exposes resources of a node
  - **Resource Directories** (with a bridge to DNS-SD)

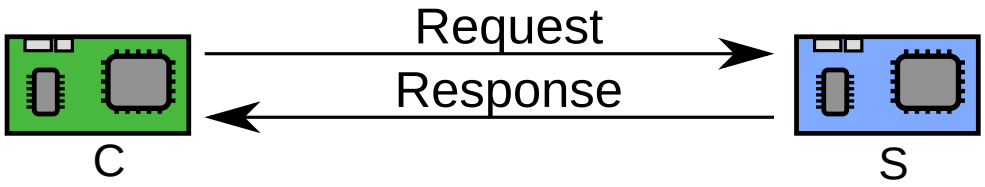
IoT Devices as a secure application

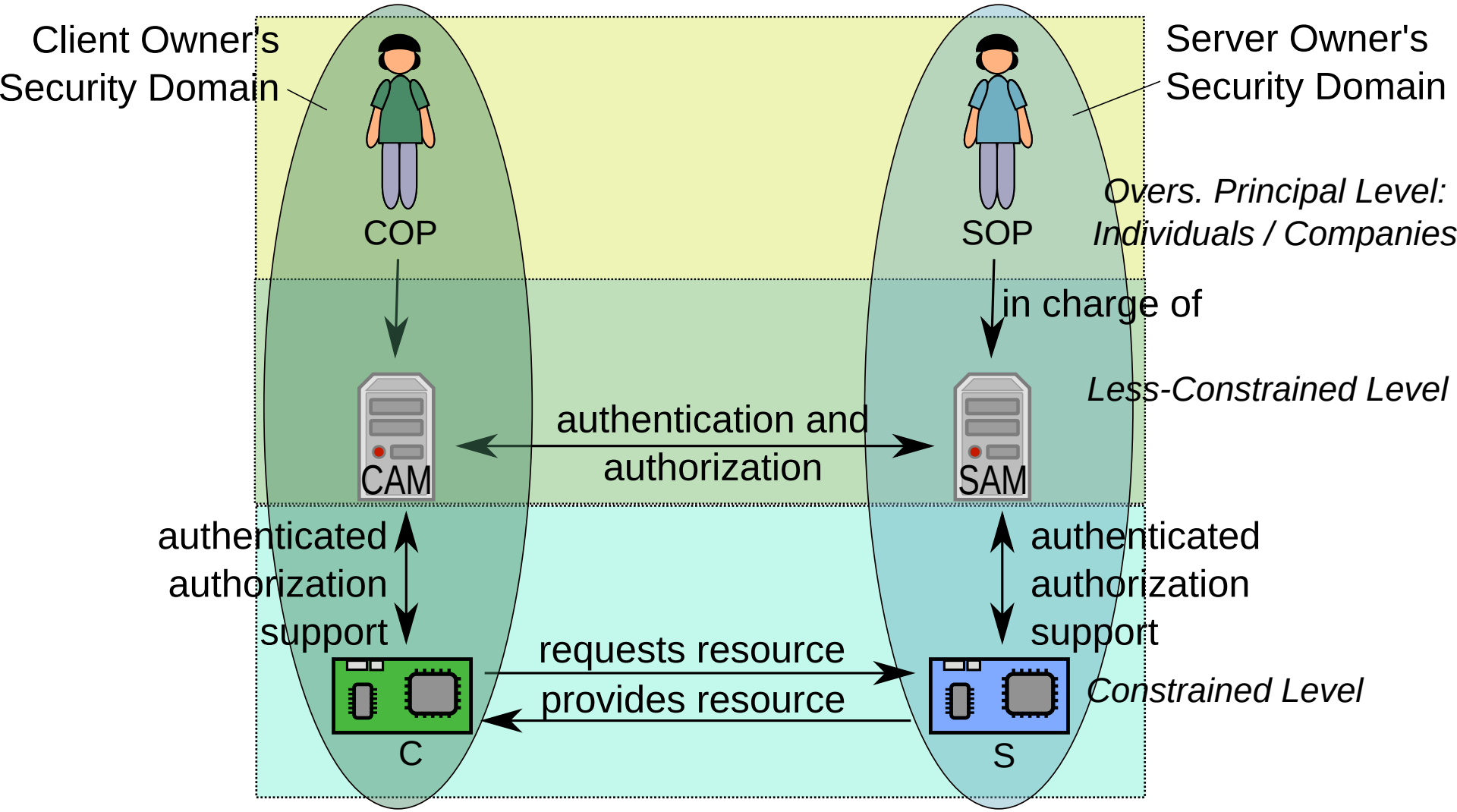
Protect the objectives right ✔

vs.

Protect the right objectives 

Now let's apply all this to constrained devices




Client Owner's
Security Domain
Server Owner's
Security Domain
COP
SOP
Overs. Principal Level:
Individuals / Companies
in charge of
Less-Constrained Level
CAM
SAM
authentication and
authorization
authenticated
authorization
support
authenticated
authorization
support
requests resource
provides resource
Constrained Level
C
S

Shaping the Security Workflows

- Stakeholders, Principals
- Less-constrained nodes
- Constrained nodes

- Device Lifecycle
- Authorized, authenticated delegation

IoT Devices as an attack platform

user duty

garage?

28

vendor duty

CE • *regulation?* • UL

29

jails

Manufacturer's Usage Description (MUD)

- Protect the network and other **unrelated** users against an IoT Device that may be insecure
- Idea: Document **expected behavior** in an actionable way
- MUD as standardized today:
  Can be used for **firewall** configuration
  - Poke firewall holes for desirable traffic
  - **Detect** when the IoT Device has been compromised
- Where can we take this idea?

Software Updates are needed

- Bugs are being found
- Environments change

→ Update or discard!

- Traditional: manual upgrade by connecting a special upgrader device (e.g., PC with upgrader app)
  - Too expensive; device might be hard to reach
- Needed: **Secure** Over-the-air Upgrade

If it is not **usably secure**,
it's not
the **Internet of Things**

I E T F®